



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/398,876	09/20/1999	UWE HANSMANN	12640(GE998-	1606

7590 07/09/2004

RICHARD L CATANIA
SCULLY SCOTT MURPHY & PRESSER
400 GARDEN CITY PLAZA
GARDEN CITY, NY 11530

EXAMINER

MCARDLE, JOSEPH M

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 07/09/2004

12

Please find below and/or attached an Office communication concerning this application or proceeding.

fr

Office Action Summary

Application No.

09/398,876

Applicant(s)

HANSMANN ET AL.

Examiner

Joseph McArdle

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 4-15-2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 8-10,23,24,33,34,39 and 40 is/are allowed.
- 6) ☒ Claim(s) 1-7,11-22,25-32,35-38 and 41-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other:

DETAILED ACTION

The Amendment received on 4/15/2004 has been received and acknowledged.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-7, 11-16, 17-22, 25-32, 35-38, and 41-43 are rejected under 35 U.S.C. 102(b) as being anticipated by Takashima (EP 0715242 A1). In regards to claims 1, 14, and 41, Takashima discloses in column 2, lines 35-39, a process by which digital information is encrypted and sent from an information center to an information terminal device. This meets the first limitation set forth under claims 1, 14, and 41, which call for transmitting an information unit in an encrypted format from a first issuer to a first processing device. Takashima further discloses in column 2, lines 39-45 that a work key (encryption/decryption key) is transmitted between the information center (issuer) and the information terminal device (processing device) for the purposes of allowing a user to decrypt the digital information that was transmitted. This disclosure meets the remaining limitations set forth under claims 1, 14, and 41, which call for providing/transmitting at least one key to be used for decryption on the second information processing device (which is the information terminal device in the Takashima reference) that can be transferred between the information processing devices for the purpose of cryptographically reprocessing the transmitted information.
2. In regards to claims 2, 15, and 42, Takashima discloses in column 2, lines 35-39, a process by which digital information is encrypted via a work key (encryption key) and

sent from an information center to an information terminal device. This meets the first limitation set forth under claims 2, 15, and 42, which call for encrypting information through the use of a first key. Takashima then discloses in column 2, lines 32-33 that the work key is encrypted according to a random number (which can be representative of a second key). This disclosure meets the second limitation set forth under claims 2, 15, and 42, which call for encrypting the first key with a second key. Takashima then goes on to disclose in column 2, lines 39-45 that the transmitted information is decrypted at the information terminal device according to the same keying method with which it was encrypted. This disclosure meets the remaining limitations set forth under claims 2, 15, and 42, which call for allowing the encryption process to be reversed by the second information processing unit.

3. In regards to claims 3, 16, and 43, Takashima discloses in column 2, lines 45-50 that an encrypted information receipt signature and work key signature are sent from the information terminal device to the information center. This disclosure meets the limitations set forth under claims 3, 16, and 43, which call for having an information processing device generate a signature for verifying the information unit according to at least one transferred key (in this case the encrypted signature results from the disclosed work key). Figure 1 meets the remaining limitations set forth under claims 3, 16, and 43, as it depicts the interconnections between the information processing devices.

4. In regards to claims 4 and 19, Takashima discloses in column 2, lines 39-45 that the transmitted information is decrypted at the information terminal device (first

information processing device) according to the same keying method with which it was encrypted. This disclosure meets the exact limitations set forth under claims 4 and 19.

5. In regards to claims 5 and 20, Takashima discloses in column 5, lines 8-16 that the information terminal device (first information processing device) contains control means for communicating with the information center in order to initiate the transfer, encryption/decryption and signature verification of the digital information. This disclosure meets the exact limitations set forth under claims 5 and 20, which call for allowing the first information processing device to provide control commands to the second information processing device in order to initiate the decryption of the first key and/or initiate the transfer of the signature key.

6. In regards to claims 6 and 21, Takashima discloses in figure 1 and in column 5, lines 36-38 that a work key for encrypting the desired digital information is provided by the information center. This meets the limitations set forth under claims 6 and 21, which call for allowing a central server (information center) to distribute encryption keys.

7. In regards to claim 7, Takashima discloses in column 5, lines 24-27 that the information terminal device (second device) contains a storage means for storing the secret key which is used in the decryption of the work key. This disclosure meets the exact limitations set forth under claim 7.

8. In regards to claims 11 and 25, Takashima discloses in column 2, lines 32-33 that the work key is encrypted according to a random number. The use of this random number allows for the first key to be randomized between different sessions of providing

the information unit from the issuer to the first device. This meets the exact limitations set forth under claims 11 and 25.

9. In regards to claims 12, 13, 26, and 27, Takashima discloses in figure 1 the use of a terminal device (which in this case is a chip card reader) and a portable device (which in this case is a chip card). This meets the exact limitations set forth under claims 12, 13, 26, and 27.

10. In regards to claims 17 and 29, Takashima discloses in column 5, lines 39-53 that encryption is used to protect information that is in transit. Takashima further discloses in the aforementioned location that the computer card contains means to encrypt and decrypt the desired information. This disclosure meets the limitations set forth under claims 17 and 29, which call for having access control being controlled by an information unit (which in this case the access control is the encryption of the information through the use of the computer card).

11. In regards to claims 18 and 30, Takashima discloses a central processing unit (CPU) in figure 3 that is maintained in the information handling terminal device. This meets the limitations set forth under claims 18 and 30, which call for having a processor run functions on a terminal device.

12. In regards to claims 22 and 32, Takashima discloses in column 9, lines 3-9 and in figure 4, that a computer card registers its key into a write only register that is protected and cannot be read out freely. This meets the limitations set forth under claims 22 and 32, which call for storing keys in a non-erasable storage.

13. In regards to claims 28 and 35, Takashima discloses in figure 1, and in column 2, lines 8-14 a computer card (chip card) that is capable of interacting with an information terminal device (information handling terminal device) for the purposes of accessing digital information. Takashima further discloses in column 2, lines 38-45 that a work key (encrypting key) is sent to the information terminal device so that the desired digital information can be decrypted. These disclosures by Takashima meet the limitations set forth under claims 28 and 35, which call for having a chip card that securely handles an information unit by interacting with an information handling terminal device (see column 2, lines 8-14) and also for providing a means to transmit at least one key to the information handling terminal in order to enable the information handling terminal to cryptographically process the information unit (see column 2, lines 38-45)

14. In regards to claim 31, Takashima discloses in column 9, lines 45-50 that the computer card is capable of transmitting its public key, identifier, and certificate to the information terminal device for authentication and verification purposes as well as for decryption purposes. This meets the limitations set forth under claim 31, which call for allowing for the chip card to transmit keys to be used either in the authentication and verification process or the information decryption process.

15. In regards to claim 36, Takashima discloses in column 5, lines 42-44 that the information handling terminal device (card accepting device) has a means to decrypt information by using a key. This meets the exact limitations set forth under claim 36.

16. In regards to claim 37, Takashima discloses in column 14, lines 50-58 how the information handling terminal device (card accepting device) applies a hash algorithm to

the received encrypted information. The chip card then uses the results of this hash in order to verify the digital signature. This meets the limitations set forth under claim 37, which calls for having a chip card device that comprises a means to verify a digital signature.

17. In regards to claim 38, Takashima discloses in figure 1, and in column 2, lines 8-14 a computer card (chip card) that is capable of interacting with an information terminal device (information handling terminal device) for the purposes of accessing digital information. Takashima further discloses in column 2, lines 38-45 that a work key (encrypting key) is sent to the information terminal device so that the desired digital information can be decrypted. These disclosures by Takashima meet the limitations set forth under claim 38, which call for having a chip card that securely handles an information unit by interacting with an information handling terminal device (see column 2, lines 8-14) and also for providing a means to transmit at least one key to the information handling terminal in order to enable the information handling terminal to cryptographically process the information unit (see column 2, lines 38-45). Takashima then discloses in column 5, lines 42-44 that the information handling terminal device (card accepting device) has a means to decrypt information by using a key. This meets the exact limitations set forth under claim 38 that call for decrypting the information unit using at least one key. Takashima then discloses in column 14, lines 50-58 how the information handling terminal device (card accepting device) applies a hash algorithm to the received encrypted information and how the chip card then uses the results of this hash in order to verify the digital signature. This disclosure meets the limitations set

forth under claim 38 that call for having a means to verify a digital signature. The final limitation set forth under claim 38 which calls for downloading the encrypted information unit, at least one key and the digital signature from a central server is met by the aforementioned disclosures because the information center (as depicted in figure 1 and described in the above rejections) is capable of providing all of the aforementioned limitations.

Response to Arguments

18. The applicant argues that that goals and preferred embodiments of the present invention are different from those of the cited Takashima reference. The examiner asserts that the claims are interpreted in light of the specification, However, the aforementioned claim rejections are based solely on the plain language of the claims.

Allowable Subject Matter

19. Claim 8-10, 23-24, 33-34, and 39-40 allowed. Independent claims 8, 23, 33, and 39 identify the uniquely distinct feature of "providing a third key for external authentication and/or release control of the respective information unit." The closest prior art Takashima (EP 0715242 A1) discloses a design that pertains to protecting digital information. However, Takashima's design makes no specific mention of the aforementioned limitation.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Joseph McArdle
Examiner
Art Unit 2132

jmm

Justin Darrow
JUSTIN T. DARROW
PRIMARY EXAMINER